IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for providing computer security, comprising:

providing an executable associated with a static state;

determining whether the executable meets a predetermined criterion; ~~and~~

associating a first risk level with the ~~criterion~~ executable, if it is determined that the executable meets the predetermined criterion;

allowing the executable to execute if the first risk level does not exceed a threat detection threshold;

updating the first risk level to a second risk level that is higher than the first risk level if a process associated with the executable is observed to perform or attempt an action with which the second risk level is associated; and

performing a predetermined responsive action with respect to one or both of the process and the executable if the second risk level exceeds the threat detection threshold;

wherein determining whether the executable meets [[a]] the predetermined criterion does not compare the executable with a virus signature.

2. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1,wherein the risk level indicates a level of potential risk that will be brought by operating the executable.

3. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the risk level indicates how much risk the executable presents.

4. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a configuration criterion.

5. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured as a service.

6. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured to run under a highly privileged account.

7. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is installed via a standard procedure.

8. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has sufficient access control.

9. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is ~~recent~~ modified.

10. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is signed.

11. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has a modified date different from created date.

12. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a capability criterion.

13. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has networking capability.

14. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has privilege manipulation capability.

15. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has remote process capability.

16. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has process launching capability.

17. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has secure coding violation.

18. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising associating with the executable a risk type indicating a type of risk to which the executable is vulnerable.

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence.

30. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a record of activities.

31. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a log file.

32. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a system optimization file.

33. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a crash dump file.

34. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a prefetch file.

35. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising performing a dynamic risk analysis.

36. (Currently amended) [[A]] The method for providing computer security as recited in Claim 1, further comprising determining whether an action is required.

37. (Currently amended) A system for providing computer security, comprising:

a processor configured to:

provide an executable associated with a static state;

determine whether the executable meets a predetermined criterion; ~~and~~

associate a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

allowing the executable to execute if the first risk level does not exceed a threat detection threshold;

updating the first risk level to a second risk level that is higher than the first risk level if a process associated with the executable is observed to perform or attempt an action with which the second risk level is associated; and

performing a predetermined responsive action with respect to one or both of the process and the executable if the second risk level exceeds the threat detection threshold;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature; and

a memory coupled with the processor, configured to provide the processor with instructions.

38. (Currently amended) A computer program product for providing computer security , the computer program product being embodied in a computer readable medium and comprising computer instructions for:

providing an executable associated with a static state;

determining whether the executable meets a predetermined criterion; ~~and~~

associating a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

allowing the executable to execute if the first risk level does not exceed a threat detection threshold;

updating the first risk level to a second risk level that is higher than the first risk level if a process associated with the executable is observed to perform or attempt an action with which the second risk level is associated; and

performing a predetermined responsive action with respect to one or both of the process and the executable if the second risk level exceeds the threat detection threshold;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature.